[2345/208]

CONTENT AND SECURITY PROXY IN A MOBILE COMMUNICATIONS SYSTEM

The present invention relates to a method and a device for making available security functions during the transmission of data from or to a subscriber terminal unit of a mobile communications network.

Current and new data services offer subscribers of mobile communications networks direct access to the Internet and other public data networks. Therefore, the mobile telephone used for mobile application, and ancillary equipment driven by it, such as a notebook or a personal digital assistant, are at the mercy of the most varied attacks by third parties, similar to what happens in a fixed network-based Internet access.

It is the object of the present invention to state a method and a device for making available security functions in the transmission of data from and to a subscriber terminal unit of a mobile communications network, so as to effectively protect the subscriber terminal unit and units connected to it or combined with it.

This object is attained by the features of the independent claims. The crux of the present invention is, in a cellular mobile telephony network, to offer a security service that is able to be personalized, individually per cellular mobile telephony connection and subscriber.

The subscriber may adjust his security settings interactively or dynamically.

The network operator may specify a series of meaningful standard settings for the filter functions, such as virus protection, protection from advertising mail, etc.

In this context, the protective function is offered by a network-specific device in the form of a security and filtering device. In addition, the general protective function may be coupled with a memory function, i.e. parts of the data traffic are temporarily stored in the device, and may be retrieved by the subscriber. Consequently, the security and filtering device may additionally take over the function of a so-called proxy. „Proxy" means as much as „representative service". Proxies accept requests from a client, for instance, a terminal unit, and pass them on, possibly modified, to the original destination, such as an Internet supplier. Proxies are able locally to file data that are passed through and to deliver them upon the next access.

With that, at the same time, one achieves an increased performance, since certain contents may be buffered.

According to the present invention, the following protective functions may be offered by the system described:

Filtering of the data traffic on an IP/TCP basis in the form of a so-called firewall function. Furthermore, filtering/refusing data packets of a certain origin (IP address) or data packets from and to certain services (TCP ports).

An analysis of the data content for contents that are malicious or critical to security. The entire content of a data connection is analyzed and searched according to certain patterns. Signatures of viruses, etc, are tracked down and rendered harmless before they reach the terminal unit of the subscriber.

An analysis of the data content for undesired subject matter, such as in the form of spam, advertising or offensive material. For this, the entire content of the connection is analyzed and content stated by the subscriber as being undesired is filtered out, for instance, to protect children and juveniles.

The network operator himself is able to use the mechanisms of the system in order purposefully to cut out, for certain subscribers, certain data traffic, such as services liable to costs, if the subscriber has not subscribed to this service.

The filtering function for the data content may be enhanced meaningfully and technically, using the same mechanisms additionally using the following functions.

For example, a limiting of the data transfer volume is relatively easy to implement. To do this, the entire traffic, under certain circumstances separated into incoming and outgoing traffic, is summed up, and additional traffic is stopped if the limit specified by the user or operator is exceeded.

In addition, budget compliance may be checked, using one component to calculate the compensation. The subscriber or the operator may specify a certain upper limit for communications cost. If the established budget is exceeded, the subscriber is notified and the data traffic is stopped. This makes possible an effective cost control and cost transparency.

Additional functions may be integrated into the system in a meaningful way:

If certain events occur, i.e. if attacks are detected, spam mails are filtered or similar events are recognized by the system, notification is made of the subscriber or network operator, in order to enable a transparent control of the data filtered out.

The subscriber may also decide administratively whether his entire traffic should be conducted over the system or only selectively, i.e. at certain times, according to specific incidents or upon suspicion of misuse.

According to one refinement of the present invention, a distributed implementation of the filter functions may be provided, i.e. the security and filter device is not provided centrally in one network node of the mobile communications system, but rather in a distributed manner, or individually in a plurality of network nodes. The load on a single node is reduced thereby.

This device of the system may

a) be conditioned spatially or upon network technology, i.e. distribution to several networks or network nodes, or

b) be conditioned functionally, for instance, special filter components for certain data contents, and, for example, email filters, virus filters, etc, or

c) conditioned upon architecture or software technology, based, for example, on the use of special hardware and system software for certain functions.

The administration of these additional functions may be performed in each case centrally, from a certain node.

An exemplary embodiment of the present invention is explained below, in the light of a drawing.

Figure 1 schematically shows the technical design of the system.

The system is a part of a mobile communications network 10, which premits a multiplicity of subscriber terminal units 13 communications with other public networks, such as the Internet 11. Furthermore, combined units 14, such as PC, PDA, Smartphone, etc, that are connected to cellular mobile telephony terminal unit 13, may be provided, which make possible a comfortable, mobile Internet use.

Security and filter device 1 is situated within mobile communications network 10, preferably within an appropriate network node, such as an exchange MSC, and, according to the present invention, it may be made up of the following functional parts.

General filter component 2:
This component has a variable filtering function specifiable by the subscriber/network operator, and it analyzes in real time the data flow 12 exchanged between terminal unit 13 of the subscriber and Internet 11. Subscriber traffic 12 in both directions goes via this filter 2 and is analyzed there.

Authentication component 3:
In order to use security and filtering device 1, the subscriber has to authenticate himself vis-a-vis the system. Thereby it is ensured that no unauthorized access can take place to, for instance, the personal settings of the subscriber. In the simplest case, the authentication may occur via call number MSISDN of the subscriber. The subscriber is protected more securely and better by the use of an additional PIN or a password. If necessary, a cryptographic authentication method may be used, e.g. certificates of the subscriber.

Administrative component 4:
This component forms the interface between the system and the

subscriber. Here the subscriber may administer his personal settings. This can be done directly via the cellular mobile telephony system, the Internet or fixed network-based customer interfaces of the network operator.

Database 5:

Database 5 describes which data are to be filtered out by filtering component 2 or are to be processed. This database 5 may advantageously be split up into four databanks. First databank 6 includes the individual filter and settings per subscriber. Second databank 7 includes the filter and settings per mobile phone type.

Third databank 8 includes the network operator-specific settings and filter, and fourth databank 9 includes the general settings and filter.